REMARKS

By this response, claims 1, 3-58 and 90-101 are pending. Compared to prior versions, all claims appear as originally or previously presented. Substantively, all claims stand rejected as anticipated by Dean (U.S. Patent No. 6,023,762) or as obvious combinations in view of Dean and French (U.S. Patent No. 5,794,228). Dean, however, is the primary patent upon which all rejections stand, with the exception that French is cited for the proposition of showing storage of multiple user objects for multiple users. In view of the following, the Applicant requests reconsideration.

Among other things, Dean teaches callers (e.g., boss, colleague, wife, self, etc.) being able to access remote data of users (e.g., employee info 200, project info 201, private info 202, etc.) apportioned amongst various "data views." Via the functionality of a gatekeeper, described as an Agent 107, callers make requests for the data and, if authenticated, the agent returns the requested data. In this regard, the agent 107 "allows or denies access to portions of data stored in the user data sources depending upon who is requesting the information and the type of data requested to be accessed." *Col. 4, ll. 39-42.* In various embodiments, the components enabling this functionality include, in general, an authorization decoder 400, a look up table 401, and a data access/retrieval signal generator 402. In turn, the look up table 401 is a "data structure" comprising:

> types of callers who may request information from the user database, and for each caller type, sets of data files or types of data files in the user data sources which can be accessed by that category of caller, together with a corresponding authentication method, corresponding to a respective level of authentication. *Col. 5, ll. 41-47.*

Naturally, portions or entireties of the underlying "information from the user database," such as "personal medical information and personal financial results" (col. 5, l. 67 - col. 6, l. 1), is populated by the user himself or herself.

Notwithstanding this teaching, Dean falls far short of anticipating or rendering the claims obvious. For example, the instant claims all require the notion of: 1) multiple profiles of multiple users being shared amongst one another upon user initiation; 2) each of the multiple profiles being stored in safes; 3) each of the safes being stored in vaults; 4) access rights of the vault going to a system administrator to manage the safes in the vaults; and 5) access and administration rights of the multiple profiles of underlying data in the safes, managed by the system administrator, going exclusively to the end users at the exclusion of the system administrator. Unequivocally, Dean never mentions the intricate level of multiple profiles being in a safe, in turn, in a vault, much less mentioning the access to manage the vault going to a system administrator with access and administration rights extending to end users ***at the exclusion of the system administrator***.

To the extent the Examiner likens Dean's agent 107 as the claimed system administrator, the Dean agent 107, contrary to the invention, **has access** to the underlying data of users being requested by callers. At Dean's step 606, Figure 6, for example, and via the functionality of the Data Access/Retrieval Signal Generator 402, the agent 107 actually does the sending of "requested info over WAN." As more precisely stated at *col. 7, ll. 54-57*, if the agent authorizes the caller, "in step 606, the authentication decoder authorizes the data retrieval signal generator ***to access the information from the user data sources*** to be sent to the service terminal [of the caller making the request]." In other words, Dean's agent simply keeps a protective gate in front of the underlying data to prevent unauthorized callers from having access to it. But, to the extent the callers have an appropriate level of access, and can authenticate it, the agent indeed fetches the underlying data and gives it to them.

This is hardly, then, the "exclusion" of a system administrator from underlying data in profiles, in safes, in vaults as the claims of the invention require. As the Examiner will recall, claims 1 and 3-58 precisely recite this functionality as follows:

> 1. (Previously Presented) A computer server system for managing digital identity information, comprising at least one processor in operable connection with a memory configured by a database, the database including a vault for storage of multiple user objects for multiple users, the vault having access rights granted to a system administrator for management of the multiple user objects, each of the user objects having a corresponding safe object, **the safe object containing multiple profiles accessed and administered exclusively by a single one of the multiple users *at the exclusion of the system administrator***, each profile including digital identity information provided by the single one of the multiple users and operable to be shared with other of the multiple users having other multiple profiles accessible and administered exclusively by the other of the multiple users, the sharing occurring exclusively upon initiation by the single one of the multiple users.

In claims 90-97 it is found as:

> 90. (Previously Presented) A computer server system for managing digital identity information, comprising one or more processors in operable connection with one or more memories defining a vault for storage of one or more safes of digital identities, the vault including an access protocol layer, an identity server layer and an identity manager layer and having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users, the one or more safes of digital identities having multiple profiles each **with access rights granted exclusively to the end users via the one or more accounts *including the exclusion of access rights of the one or more system administrators***, the multiple profiles

> being shared amongst the end users at the exclusion of the one or more system administrators.

While claims 98-100 require it as:

> 98. (Previously Presented) A configured computer-readable storage medium that manages digital identities, comprising a vault for secure storage of one or more safes of digital identity profiles, the vault having an access protocol layer, an identity server layer and an identity manager layer and having **access rights granted to a system administrator for management of the safes of digital identity profiles, the one or more safes of digital identity profiles having access rights granted *exclusively* to one or more end users at locations remote from the vault**, the one or more safes of digital identity profiles further including multiple profiles shared amongst the end users at the exclusion of the system administrator.

For this reason alone, reconsideration of all claims is certainly appropriate.

Nonetheless, the Examiner further rejects the claims by making associations to the prior art that, quite frankly, do not exist anywhere in the teachings. For example, the Examiner rejects claims 90-101 by associating the "identity server layer" of the claims with Dean's element 803, Figure 8. *See, 1-3-06 Office Action, page 3, ll 5-6.* However, element 803 of Figure 8 recites a step of a service terminal as "Send terminal ID signal to key device." Without a doubt, this does not and cannot equate to a precisely claimed software abstraction "identity server layer," especially one in a "vault" further including "an access protocol layer . . . and an identity manager layer." At best, the rejection is only plausible upon a further, forthcoming explanation by the Examiner. At worst, the rejection is a disingenuous attempt to unfairly, and unconstitutionally, prevent the Applicant from issuing a patent for the given subject matter.

Similarly, the "exclusive" administration by users in claims 1 and 3-58 is purportedly found in Dean by the following: "(each user, without the system administrator, configures look-up table [sic] (for safe object access))." *1-3-06 Office Action, p. 8, ll. 5-6.* The Applicant, however, does not dispute Dean teaches users configuring underlying information in a look up table. But, to suggest that Dean's system administrators, to the extent an agent 107 is arguably a system administrator, renders obvious or anticipates the invention, is failure, as a matter of law. Surely, this rejection is either 1) plausible only upon a further, forthcoming explanation by the Examiner or 2) is a disingenuous attempt to equate a reference to the claims where no equation exists. As before, nowhere does Dean suggest that its agent 107 is excluded from information of the look up table. In fact, it is the exact converse. Especially, Dean's agent 107 not only has access to the underlying information of the look up table, but 1) retrieves it (via the functionality of device 402) and 2) provides it to authenticated callers, e.g., step 606. Also, the Examiner has never clarified the record as to why an agent 107 of Dean should even be equated to a system administrator of the claims. For at least these reasons, reconsideration of the patentability of the claims is further appropriate.

Regarding French, the Applicant submits its combination with Dean is entirely unfounded and inappropriate. French broadly teaches data compression and decompression. It has nothing at all to do with managing digital identities, like the invention. It has nothing at all to do with Dean's intermediary agent 107 that gate-keeps information from callers. It is simply being cited for selectively culled pieces of the prior art that the Examiner contends is necessary in rejecting the claims.

Respectfully, the Applicant respectfully reminds the Examiner that it is impermissible to utilize hindsight reconstruction when examining the claims. The proper test of obviousness is whether the differences between the invention and the prior art are such that

"the subject matter as a whole would have been obvious at the time the invention was made" to a person skilled in the art. *Stratoflex Inc. V. Aeroquip Corp.*, 713 F.2d 1530, 1538 (Fed. Cir. 1983)(Underlining added). Bear in mind, the Applicant originally filed for patent protection on September 27, 2000. It is now over five full years since filing. The Applicant also reminds the Examiner of caution expressed by the Court of Appeals for the Federal Circuit that "[d]etermination of obviousness can not be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the [] invention." *ATD Corp. v. Lydall, Inc.*, 159 f.3d 534, 536 (Fed. Cir. 1998).

Unfortunately, the prosecution of this case appears to be that of an Examiner finding somewhat irrelevant references and applying the same in rejecting the claims. Further unfortunately, the last time this occurred, the Applicant filed a thoughtful response. However, the Examiner issued a final, premature rejection and did so on an erroneous record built on non-existent claim limitations about "the string" of something. After filing an RCE, the Examiner again searched and is applying more art that certainly should have been found in previous searches. Naturally, the cost of prosecution to Applicants is generally expensive in modern times, but the cost in this matter has progressed seemingly unfairly for reasons unbeknownst to the Applicant. It is, thus, with great respect the Applicant requests reconsideration of the claims in view of the foregoing comments. The burden on the Applicant to continually fend off imprecise reasoning is, as can be appreciated, overly costly.

Still further, each of the claims distinguish themselves over the art of record for, at least, the following reasons:

Claim 1 requires a database having a vault for storing multiple users objects of multiple users. In turn, the user objects have safe objects which contain "multiple different profiles" of the users that are accessed and administered exclusively by the users, at the exclusion of the system administrator, and are able to be shared with one another. Dean,

however, describes an agent 107 that accesses underlying data and provides it to authorized callers. French, on the other hand, adds nothing of relevance to the Dean reference;

Claim 90 requires a vault "having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users" and "one or more safes of digital identities" in the vault "having access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators." In other words, without restricting the claim scope beyond the words expressly recited, administrators have access rights to vaults and to the management of the accounts of end users. End-users have exclusive access rights to their digital identities in the vault, yet obtained these rights via their accounts, in turn, managed by the administrator. In still other words, end users have access to the substance of underlying data of their digital identities while administrators give the end users their ability to get to the substance. Neither Dean nor French teach such a system. Further, the claim requires various abstraction "layers" that are nowhere found in the references in the manner recited by the claims;

Claim 98 requires access rights to the vault be given to system administrators while access rights to the multiple digital identity profiles, stored in the vault, be given to end users exclusively. Also, the claim requires "layers." Again, Dean does not teach this and French adds nothing of value, in this regard.

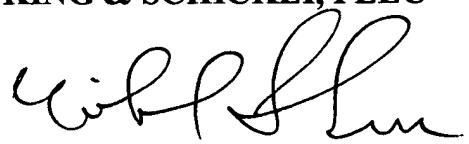
The entirety of the dependent claims are submitted as being patentable because of their dependence on one of claims 1, 90 or 98 discussed above. Of course, additional reasons of patentability can be given but are being held in abeyance in anticipation of a Notice of Allowance.

The Applicant submits all claims are in a condition for allowance and requests a timely Notice of Allowance be issued for same. ***To the extent any fees are due, although***

none are believed due, the undersigned authorizes their deduction from Deposit Account No. 11-0978. Finally, the Applicant requests a change in the attorney document number of record. Namely, please replace 1909.2.74A with 1363-006. The docket number changed when the new Power of Attorney (POA) went into effect.

Respectfully submitted,

KING & SCHICKLI, PLLC



Michael T. Sanderson
Registration No, 43,082

247 North Broadway
Lexington, Kentucky 40507
Phone: (859) 252-0889
Fax: (859) 252-0779

Certificate of Mailing
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on February 10, 2006
Date 2/10/06 by